IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

UNITED STATES OF AMERICA, v. JOHN CHARLES WILLARD, JR., Defendant.	Action Number 3:10-CR-154

MEMORANDUM OPINION

THIS MATTER comes before the Court on the following motions by John Charles Willard, Jr. ("Defendant"): (1) a Motion to Suppress Statements; (2) a Motion to Suppress Evidence; (3) a Motion to Qualify Expert Witness; and (4) a Motion for a Franks Hearing. The parties appeared before this Court for a hearing on September 14, 2010. For the reasons stated from the bench and below, Defendant's motions are all DENIED.

BACKGROUND

An undercover agent working for the Federal Bureau of Investigation ("FBI") conducted a keyword search on a peer-to-peer file-sharing network using terms known to be associated with child pornography. Her search revealed a file from Internet Protocol ("IP") address 24.125.166.216. The FBI agent conducted a search of other files available at this IP address and downloaded seven files, three of which depicted child pornography. Special Agent George Howell of the FBI subsequently viewed the images and confirmed

that they depicted child pornography. After being served with a subpoena, Comcast Corporation identified the owner of the IP address as John C. Willard, Sr., a resident of Mechanicsville, Virginia.

On September 11, 2008, United States Magistrate Judge M. Hannah Lauck authorized the installation of a pen register device on the Internet connections of both John C. Willard, Sr., and Defendant, who had recently moved out of his father's home.

In 2009, Special Agent Howell analyzed the pen data using the Wyoming Toolkit database.[1] The database uses an automated software program called Peer Spectre which reads publicly available information from computers identified as sharing child pornography images. Special Agent Howell queried Wyoming Toolkit regarding the IP addresses that communicated with Defendant's IP address in October and November 2008, and found that more than 2,200 of those IP addresses had been previously identified by Peer Spectre as advertising child pornography files available for sharing.

In the spring of 2009, another judicially-authorized pen register was installed on Defendant's Internet connection. Analysis of Defendant's Internet activity revealed that Defendant's IP address made thirty unique files of child pornography available for sharing on four separate occasions between May and July of 2009.

---

[1]The Wyoming Toolkit database was developed by the Wyoming Internet Crimes Against Children ("ICAC") Task Force. Whenever an investigator identifies child pornography that is shared over a peer-to-peer file-sharing network, the observation is recorded into the Wyoming Toolkit database. The database record contains: (1) the date and time of the observation; (2) the SHA1 value of the files; and (3) the name of the files and the IP address sharing the files. SHA1 stands for Secure Hash Algorithm 1. It is essentially a fingerprint of a digital file. By comparing the SHA1 values of two files, investigators can determine whether the files are identical with precision greater than 99.9999 percent certainty.

On August 26, 2009, Special Agent Howell obtained a search warrant for Defendant's address authorizing the search and seizure of Defendant's computer and related items. The search warrant was executed August 27, 2009. Officers seized Defendant's computer, along with its hard drive, and an external hard drive. A subsequent analysis of the hard drives revealed more than 300 still images and 67 videos of child pornography.

When the officers arrived to execute the search warrant, they identified themselves, and asked Defendant if he would answer questions related to the child pornography investigation. Defendant agreed. The officers advised Defendant that he was not under arrest and was free to leave. The officers also presented Defendant with an Advice of Rights form, which Defendant signed after indicating he understood his rights. The officers then interviewed Defendant in a sport utility vehicle. During the interview, Defendant admitted to using the LimeWire peer-to-peer file sharing program to download pornography and told the officers he was mainly interested in pornography featuring "barely legal" teenagers. He claimed no interest in "hardcore" pornography and, when asked about sexually explicit online posts pertaining to incest activities with minor daughters that he admitted to making in 2008, Defendant said he had not written anything of that nature since 2008.

Defendant now argues: (1) evidence obtained during the child pornography investigation should be suppressed because the pen register installed on his Internet connection was actually a wiretap that required a search warrant based on probable cause and (2) the incriminating statements he made to the officers should be suppressed because

the waiver of his Miranda rights was not voluntary and was ineffective because the officers read him his rights after he made the statements. Further, he seeks a Franks hearing and would like to have his father qualified as an expert witness.

DISCUSSION

A. Motion to Suppress Evidence

A "trap and trace" device is defined as "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication...." 18 U.S.C. § 3127(4). A "pen register" is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted...." 18 U.S.C. § 3127(3). When using a pen register or trap and trace device on a computer, the government is not entitled to receive information from the device if that information reveals the contents of a communication. In re United States for an Order Authorizing the Use of a Pen Register & Trap, 396 F. Supp. 2d 45, 47 (D. Mass. 2005). See also 18 U.S.C. § § 3127(3)-(4).

A court must enter an order authorizing the installation and use of a pen register or trap and trace if it finds that an attorney for the Government has certified that "the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation." 18 U.S.C. § 3123(a)(1). A government agency authorized to install and use a pen register or trap and trace must use reasonably available technology "that restricts the recording or decoding of electronic or other impulses to the dialing, routing,

addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications." 18 U.S.C § 3121(c).

Defendant's primary argument is based on the fact that the pen register and trap and trace statutes allow only the collection of the origin or destination of a communication and not the contents of the communication. Defendant contends that a search that includes the opening of files exchanged between two IP addresses is beyond the scope of an order authorizing the use of a pen register or trap and trace device. Thus, Defendant argues, the orders obtained authorized a search only of information pertaining to routing, addressing and signaling. He asserts that Special Agent Howell went beyond the scope of the order when he used software to monitor the flow of information and read and record the IP address, date, time, file names, and SHA1 values of files on Defendant's computer. To have properly engaged in this type of search, Defendant contends, the Government should have obtained a warrant pursuant to the Wire and Electronic Communications Interception and Interception of Oral Communications Act, 18 U.S.C. §§ 2510-2522 ("Wiretap Act").

The Wiretap Act generally requires a party to obtain an order to intercept electronic communications. See 18 U.S.C. §§ 2511(1)(a) and 2518(1) . Any person aggrieved by the interception of communications can move to suppress the contents of communication if "(i) the communication was unlawfully intercepted; (ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or (iii) the interception was not made in conformity with the order of authorization or approval." 18 U.S.C. § 2518(10)(a).

Defendant's argument that the process used by the officers in collecting information from his computer constituted a wiretap is based on the holding in In re United States. In that case, the court opined, "...the argument could be made that any process or device that collects the content of an electronic communication is not, in fact, a pen register or trap and trace device but, instead, is an electronic intercepting device as defined in [the Wiretap Act]." In re United States, 416 F. Supp. 2d 13, 18 (D.D.C. 2006).

Defendant argues in the instant case that the Government's use of Wyoming Toolkit and Peer Spectre to determine the nature of his computer files was analogous to installing a wiretap and went beyond the scope of the pen register orders. As such, Defendant argues, the officers should have obtained a search warrant based on probable cause.

The Court finds that the use of Peer Spectre did not constitute a wiretap because the software does not intercept electronic communications. The functions performed by Peer Spectre and Wyoming Toolkit are more akin to mining data. The term "intercept" as used in the Wiretap Act requires that the acquisition of contents be contemporaneous with the transmission of such contents. See Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002) ("Congress ... accepted and implicitly approved the judicial definition of 'intercept' as acquisition contemporaneous with transmission. We therefore hold that for a website ... to be 'intercepted' in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage."). Peer Spectre does not acquire communications contemporaneously with the transfer of data from one IP address to another. Instead, it reads publicly available advertisements from computers identified as offering images of child pornography for distribution and identifies their IP addresses.

Considering the above factors, the Court finds that Defendant's motion to suppress evidence should be denied.

B. Motion to Suppress Statements

A person subject to custodial interrogation must be advised of his rights before being questioned by a law enforcement officer. Miranda v. Arizona, 384 U.S. 436, 467 (1966). "Custodial interrogation" is "questioning initiated by law enforcement officers after a person has been taken into custody or otherwise deprived of his freedom of action in any significant way." Id. at 444. Whether a suspect is in custody is an objective determination and depends on "how a reasonable man in the suspect's position would have understood his situation." Berkemer v. McCarty, 468 U.S. 420, 442 (1984). A person may waive his Miranda rights as long as he does so voluntarily, knowingly and intelligently. Miranda, 384 U.S. at 444. The burden of showing a valid Miranda waiver rests on the prosecution, which must prove the waiver by a preponderance of the evidence. Colorado v. Connelly, 479 U.S. 157, 168-9 (1986).

There must be two inquiries to determine if a defendant has effectively waived his Miranda rights: "First, the relinquishment of the right must have been voluntary in the sense that it was the product of a free and deliberate choice rather than intimidation, coercion, or deception. Second, the waiver must have been made with a full awareness of both the nature of the right being abandoned and the consequences of the decision to abandon it." Moran v. Burbine, 475 U.S. 412, 421 (1986). A court may find that a defendant waived his rights only if the totality of the circumstances indicates both "an uncoerced choice and the requisite level of comprehension." Id.

Defendant argues that his statements to the officers regarding his use of LimeWire and his interest in "barely legal" teenage pornography should be suppressed because the waiver of his rights was not voluntary. Defendant alleges that he suffers from bipolar disorder and was deprived of medication while in the officers' custody. He further asserts that he was in physical pain and not in a normal state of mind during the interrogation and that the police coerced him by taking advantage of his mental illness.

The Court finds that Defendant's waiver of his Miranda rights was voluntary and not coerced. Furthermore, Defendant's testimony regarding the officers' arrival at his home early in the morning, use of a battering ram on his door, and asking if Defendant knew why the officers were at his home does not justify suppressing the statements, as these activities did not coerce him into waiving his Miranda rights.

To be effective, Miranda warnings must be administered prior to an interrogation. Missouri v. Seibert, 542 U.S. 600, 613 (2004). "Upon hearing warnings only in the aftermath of interrogation and just after making a confession, a suspect would hardly think he had a genuine right to remain silent.... Thus, when *Miranda* warnings are inserted in the midst of coordinated and continuing interrogation, they are likely to mislead and 'depriv[e] a defendant of knowledge essential to his ability to understand the nature of his rights and the consequences of abandoning them.'" Id. at 613-14 (quoting Moran v. Burbine, 475 U.S. 412, 424 (1986)). Missouri also sets fourth several factors relevant in determining whether a midstream Miranda warning could be effective: "the completeness and detail of the questions and answers in the first round of interrogation, the overlapping content of the two statements, the timing and setting of the first and the second, the continuity of

police personnel, and the degree to which the interrogator's questions treated the second round as continuous with the first." Missouri, 542 U.S. at 615.

Defendant claims his statements should be suppressed because the Miranda warnings were ineffective, as they were read to him after he made incriminating statements. Defendant asserts that he agreed to answer the officers' questions, but was not given his Miranda warnings until after the questioning began, and that an analysis of the Missouri factors demonstrates that the Miranda warning was ineffective. He states that there was no break in questioning and that the officers made no effort to explain to him that the statements made before the warnings could not be used against him. As a result, the warnings did not lead him to a meaningful understanding that he could stop answering questions after the warnings were given. Thus, he argues, his waiver was not effective because of the timing of the warnings and because the post-Miranda questioning resulted from knowledge obtained from answers to pre-Miranda questions.

The Court credits Special Agent Howell's testimony with respect to the sequence of events on the morning the search warrant was executed. Specifically, the Court credits the officer's testimony that the officers read Defendant his rights upon arriving at his home and proceeded to interview him after Defendant indicated orally that he understood his rights and executed a waiver of rights form. As such, the Miranda warnings were effective and the Defendant's statements need not be suppressed on this ground.

C. Motion to Qualify Expert Witness

"If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise...." Fed. R. Evid. 702. "...[T]he trial judge must ensure that any and all scientific testimony or evidence admitted is not only relevant, but reliable." Daubert v. Merrell Dow Pharms., 509 U.S. 579, 589 (1993).

Defendant seeks to qualify his father, John C. Willard, Sr. as an expert witness. Defendant's justification for using his father as an expert witness is that his father is skilled in information systems. He seeks to have his father testify regarding IP addresses and their relationships to computers, the accuracy of SHA1 values, and the process of intercepting electronic communication and methods of collecting personal information which are outside the purview of an authorized pen register. Defendant asserted that his father would testify regarding certain technical flaws that would affect the facts in the affidavit used to establish probable cause for a search warrant.

The Court finds that the proposed testimony of Defendant's father would be too unreliable and denies the motion to qualify Defendant's father as an expert witness.

D. Motion for *Franks* Hearing

The Supreme Court of the United States held in Franks v. Delaware:

> Where the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable

> cause, the Fourth Amendment requires that a hearing be held at the defendant's request. In the event that at that hearing the allegation of perjury or reckless disregard is established by the defendant by a preponderance of the evidence, and, with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable case was lacking on the face of the affidavit. Franks v. Delaware, 438 U.S. 154, 155-6 (1978).

Defendant argues in the instant case that the agents incorporated false and reckless statements in the affidavit presented to obtain a search warrant for Defendant's home and that these false and reckless statements misled the judge in making the probable cause determination. Specifically, Defendant alleges that the affidavit misled the court by stating that Defendant was in fact communicating with certain IP address offering child pornography because the officers did not negate the possibility that someone else could have been using the IP address in question. Defendant further alleges that the officers making the affidavit made false statements regarding the accuracy of SHA1. Finally, Defendant argues that the affidavit redacted to exclude the allegedly false statements by the agents is not sufficient to establish probable cause for a search warrant.

This Court finds that Defendant is not entitled to a Franks hearing as none of Defendant's allegations makes the requisite preliminary showing to justify the hearing. As such, Defendant's motion is denied.

CONCLUSION

For the above reasons and for the reasons stated from the bench, the Court hereby DENIES Defendant's Motion to Suppress Statements; Motion to Suppress Evidence; Motion to Qualify Expert; and Motion for Franks Hearing.

Let the Clerk send a copy of this Memorandum Opinion to all parties of record.

An appropriate Order shall issue.

/s/
James R. Spencer
Chief United States District Judge

Entered this 20th day of September 2010